



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/056,702	01/25/2002	Victor Kouznetsov	002.0230.01	2048

22895 7590 02/09/2005

PATRICK J S INOUE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

EXAMINER

SANTOS, PATRICK J D

ART UNIT	PAPER NUMBER
----------	--------------

2161

DATE MAILED: 02/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/056,702

Applicant(s)

KOUZNETSOV ET AL.

Examiner

Patrick J Santos

Art Unit

2161

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 29 September 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-54 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-54 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Objections

1. Claims 1-23 are objected to because of the following informality: amended independent Claims 1 and 12 contain the phrase, "management of **the** each network appliance" (Amendment: p. 3, claim 1, ln. 8; p. 5, claim 12, lns. 7-8). Dependent Claims 2-11 and 13-23 inherit same deficiency. Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. Claims 1-2, 4-13, 15-23, 39-40, 44-51, and 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,256,668 issued to Slivka et al. (hereafter Slivka '668) in view of U.S. Patent Application Publication No. 2002/0184619 by Meyerson (hereafter Meyerson '619).

Claim 1:

Regarding Claim 1, Slivka '668 discloses: a system for providing a framework for network appliance management in a distributed computing environment (Slivka '668: Abstract), comprising:

- an appliance status table recording a status report periodically received from each of a plurality of network appliances, each status report containing health and status

information and application-specific data of the each network appliance (Slivka '668: col. 2, lns. 37-43; col. 3, lns. 8-13; col. 3, lns. 21-23 – note that inventory and version information reads on health, status, and application specific data); and

- a catalog server maintaining configuration settings for each network appliance progressively assembled concurrent to providing installable components (Slivka '668: col. 2, lns. 42-44 – note the update service database of reads on a catalog server) and dynamically providing a catalog listing currently installable components for each network appliance based on the configuration settings (Slivka '668: col. 2, lns. 44-52; col. 8, lns. 2-5).

However, Slivka '668 does not explicitly disclose that:

- the status report was from “a status daemon autonomously operating” on the network appliance;
- the information is “pertaining to autonomous configuration and management”; or
- the configuration settings are “independently received from the network appliance.”

Meyerson '619 discloses an intelligent update agent. Specifically, Meyerson '619

discloses:

- that the status report was from “a status daemon autonomously operating” on the network appliance (Meyerson '619: paras. [0022] and [0026] – note that the agent is completely automated and runs on the client machine and reads on an autonomously operating status daemon);
- that the information is “pertaining to autonomous configuration and management” (Meyerson '619: paras. [0028] and [0029]; paras. [0033], [0034], and [0036]); and

- that the configuration settings are “independently received from the network appliance” (Meyerson ‘619: paras. [0022] and [0026]).

It would have been obvious to a person having ordinary skill in the art to replace the user initiated update of Slivka ‘668 with the autonomous intelligent update of the Meyerson ‘619 agent. The motivation to combine is suggested by Meyerson ‘619 which discloses the advantage that a class of updates that are critical to a machine need not rely on human interaction to initiate updates such as that of Slivka ‘668 (Meyerson ‘619: paras. [0011] and [0012]).

Claims 2, 4, 7, and 10-11:

Regarding Claims 2, 4, 7, and 10-11, Slivka ‘668 and Meyerson ‘619, in combination disclose all the limitations of Claim 1 (supra). Additionally, Slivka ‘668 and Meyerson ‘619, in combination disclose:

- (Claim 2) a network operations center establishing a secure session with each network appliance (Slivka ‘688: col. 13, lns. 9-15; col. 2, lns. 65-67; col. 3, lns. 5-8);
- (Claim 4) wherein the currently installable components comprise at least one self-installable package, further comprising: a component server supplying the at least one package for installation responsive to a request from one such network appliance (Slivka ‘688: col. 13, lns. 6-8; col. 13, lns. 27-37);
- (Claim 7) wherein the installable components comprise at least one file, further comprising: a component server supplying the at least one file responsive to a request from one such network appliance (Slivka ‘688: col. 13, lns. 6-8; col. 13, lns. 27-37 – note the files comprising the installation read on at least one file);

Art Unit: 2161

- (Claim 10) a proxy component server staging the currently installable components for retrieval in a separate components database (Slivka '668: col. 5, lns. 28-37 – note the remote site reads on a staging proxy component server);
- (Claim 11) wherein the distributed computing environment is TCP/IP-compliant (Slivka '668: col. 6, lns. 26-28).

Claims 5-6:

Regarding Claims 5-6, Slivka '668 and Meyerson '619, in combination disclose all the limitations of Claim 4 (supra). Additionally, Slivka '668 and Meyerson '619, in combination disclose:

- (Claim 5) a crypto module digitally signing the at least one package for the network operations center prior to being supplied for installation (Slivka '668: col. 17, lns. 21-38);
- (Claim 6) a crypto module encrypting the at least one package prior to being supplied for installation (Slivka '668: col. 17, lns. 21-45).

Claims 8-9:

Regarding Claims 8-9, Slivka '668 and Meyerson '619, in combination disclose all the limitations of Claim 7 (supra). Additionally, Slivka '668 and Meyerson '619, in combination disclose:

- (Claim 8) wherein the component server establishes a secure session prior to the at least one file being supplied for installation (Slivka '668: col. 13, lns. 9-15; col. 2, lns. 65-67; col. 3, lns. 5-8);

- (Claim 9) a file information subdirectory specifying installation instructions for the at least one file in a pre-determined entry prior to the at least one file being supplied for installation (Slivka '668: col. 13, lns. 38-45; col. 14, lns. 15-42 – note the Media Directive File reads on installation instructions; further note the directory specification for setup.exe, i.e. the setup executable).

Claim 12:

Regarding Claim 12, Slivka '668 discloses: a method for providing a framework for network appliance management in a distributed computing environment (Slivka '668: Abstract), comprising:

- recording a status report periodically received from each of a plurality of network appliances, each status report containing health and status information and application-specific data for each network appliance (Slivka '668: col. 2, lns. 37-43; col. 3, lns. 8-13; col. 3, lns. 21-23 – note that inventory and version information reads on health, status, and application specific data);
- maintaining configuration settings for each network appliance progressively assembled concurrent to providing installable components (Slivka '668: col. 2, lns. 42-44); and
- dynamically providing a catalog listing currently installable components for each network appliance based on the configuration settings (Slivka '668: col. 2, lns. 44-52; col. 8, lns. 2-5).

However, Slivka '668 does not explicitly disclose that:

- the status report was from “a status daemon autonomously operating” on the network appliance;

- the information is “pertaining to autonomous configuration and management”; or
- the configuration settings are “independently received from the network appliance.”

Meyerson ‘619 discloses an intelligent update agent. Specifically, Meyerson ‘619 discloses:

- that the status report was from “a status daemon autonomously operating” on the network appliance (Meyerson ‘619: paras. [0022] and [0026] – note that the agent is completely automated and runs on the client machine and reads on an autonomously operating status daemon);
- that the information is “pertaining to autonomous configuration and management” (Meyerson ‘619: paras. [0028] and [0029]; paras. [0033], [0034], and [0036]); and
- that the configuration settings are “independently received from the network appliance” (Meyerson ‘619: paras. [0022] and [0026]).

It would have been obvious to a person having ordinary skill in the art to replace the user initiated update of Slivka ‘668 with the autonomous intelligent update of the Meyerson ‘619 agent. The motivation to combine is on the same basis as Claim 1 (supra).

Claims 13, 15, 18, and 21-22:

Regarding Claims 13, 15, 18, and 21-22, Slivka ‘668 and Meyerson ‘619, in combination disclose all the limitations of Claim 12 (supra). Additionally, Slivka ‘668 and Meyerson ‘619, in combination disclose:

- (Claim 13) establishing a secure session with each network appliance (Slivka ‘668: col. 13, lns. 9-15; col. 2, lns. 65-67; col. 3, lns. 5-8);

- (Claim 15) wherein the currently installable components comprise at least one self-installable package, further comprising: supplying the at least one package for installation responsive to a request from one such network appliance (Slivka '688: col. 13, lns. 6-8; col. 13, lns. 27-37);
- (Claim 18) wherein the installable components comprise at least one file, further comprising: supplying the at least one file responsive to a request from one such network appliance (Slivka '688: col. 13, lns. 6-8; col. 13, lns. 27-37 – note the files comprising the installation read on at least one file);
- (Claim 21) staging the currently installable components for retrieval in a separate components database (Slivka '668: col. 5, lns. 28-37 – note the remote site reads on a separate components database;
- (Claim 22) wherein the distributed computing environment is TCP/IP-compliant (Slivka '668: col. 6, lns. 26-28).

Claims 16-17:

Regarding Claims 16-17, Slivka '668 and Meyerson '619, in combination disclose all the limitations of Claim 15 (supra). Additionally, Slivka '668 and Meyerson '619, in combination disclose:

- (Claim 16) digitally signing the at least one package prior to being supplied for installation (Slivka '668: col. 17, lns. 21-38);
- (Claim 17) encrypting the at least one package prior to being supplied for installation (Slivka '668: col. 17, lns. 21-45).

Claims 19-20:

Regarding Claims 19-20, Slivka '668 and Meyerson '619, in combination disclose all the limitations of Claim 18 (supra). Additionally, Slivka '668 and Meyerson '619, in combination disclose:

- (Claim 19) establishing a secure session prior to the at least one file being supplied for installation (Slivka '668: col. 13, lns. 9-15; col. 2, lns. 65-67; col. 3, lns. 5-8);
- (Claim 20) specifying installation instructions for the at least one file in a predetermined entry prior to the at least one file being supplied for installation (Slivka '668: col. 13, lns. 38-45 – note the Media Directive File reads on installation instructions; further note the additional options and details for installation directives extensively detailed from col. 13, ln. 38 to col. 17, ln. 20).

Claim 23:

Regarding Claims 23, Slivka '668 and Meyerson '619, in combination disclose all the limitations of Claims 12, 13, 15, 16, 17, 18, 19, 20, 21, and 22 (supra). Additionally, Slivka '668 and Meyerson '619, in combination disclose a computer-readable storage medium implementing the limitations of Claims 12, 13, 15, 16, 17, 18, 19, 20, 21, and 22 (Slivka '668: col. 19, lns. 59-61). Slivka '668 does not disclose all the limitations of Claim 14, however Examiner notes Claim 23 was written in the alternative, thus Claim 23 with respect to Claim 14 need not be addressed.

Claim 39:

Regarding Claim 39, Slivka '668 discloses: a method for autonomously managing a network appliance deployed within a distributed computing environment, comprising:

Art Unit: 2161

- maintaining an internal catalog of components installed on one such network appliance identified by component and version (Slivka '668: col. 7, lns. 39-44; col. 12, lns. 6-32 – note the Windows (TM) registry reads on an internal catalog of components);
- periodically providing a status report containing health and status information and application-specific data for the one such network appliance (Slivka '668: col. 2, lns. 37-43; col. 3, lns. 8-13; col. 3, lns. 21-23 – note that inventory and version information reads on health, status, and application specific data);
- obtaining a catalog of currently installable components dynamically generated for the one such network appliance (Slivka '668: col. 2, lns. 42-44 – note the update service database of reads on a catalog server); and
- determining non-current components by comparing the components and versions listed in the obtained catalog against the internal catalog (Slivka '668: col. 2, lns. 44-52).

However, Slivka '668 does not explicitly disclose that:

- the status report was from “a status daemon autonomously operating” on the network appliance;
- the information is “pertaining to autonomous configuration and management”; or
- the configuration settings are “independently received from the network appliance.”

Meyerson '619 discloses an intelligent update agent. Specifically, Meyerson '619 discloses:

- that the status report was from “a status daemon autonomously operating” on the network appliance (Meyerson '619: paras. [0022] and [0026] – note that the agent is completely

automated and runs on the client machine and reads on an autonomously operating status daemon);

- that the information is “pertaining to autonomous configuration and management” (Meyerson ‘619: paras. [0028] and [0029]; paras. [0033], [0034], and [0036]); and
- that the configuration settings are “independently received from the network appliance” (Meyerson ‘619: paras. [0022] and [0026]).

It would have been obvious to a person having ordinary skill in the art to replace the user initiated update of Slivka ‘668 with the autonomous intelligent update of the Meyerson ‘619 agent. The motivation to combine is on the same basis as Claim 1 (supra).

Claims 40, 44, 49, and 53:

Regarding Claims 40, 44, 49, and 53, Slivka ‘688 and Meyerson ‘619, in combination disclose all the limitations of Claim 39 (supra). Additionally, Slivka ‘688 and Meyerson ‘619, in combination disclose:

- (Claim 40) negotiating a secure connection with the one such network appliance (Slivka ‘668: col. 13, lns. 9-15; col. 2, lns. 65-67; col. 3, lns. 5-8);
- (Claim 44) the components comprise at least one self-installable package, further comprising:
 - o obtaining the at least one self-installable package (Slivka ‘688: col. 13, lns. 6-8);
 - and
 - o installing the at least one self-installable package per instructions encoded therein (Slivka ‘688: col. 13, lns. 27-37).

- (Claim 49) the components further comprise at least one file, further comprising:
obtaining the at least one file; and installing the at least one self-installable package per instructions stored in a pre-determined entry (Slivka '668: col. 13, lns. 38-45; col. 14, lns. 15-42 – note the Media Directive File reads on installation instructions; further note the directory specification for setup.exe, i.e. the setup executable).
- (Claim 53) the distributed computing environment is TCP/IP-compliant (Slivka '668: col. 6, lns. 26-28).

Claims 45-48:

Regarding Claims 45-48, Slivka '688 and Meyerson '619, in combination disclose all the limitations of Claim 44 (supra). Additionally, Slivka '688 and Meyerson '619, in combination disclose:

- (Claim 45) the components further comprise at least one file dependent on the at least one self-installable package, further comprising: obtaining the at least one file subsequent to installing the at least one self-installable package; and installing the at least one self-installable package per instructions stored in a pre-determined entry (Slivka '668: col. 13, lns. 38-45; col. 14, lns. 15-42 – note the Media Directive File reads on installation instructions; further note the directory specification for setup.exe, i.e. the setup executable).
- (Claim 46) negotiating a non-secure session prior to obtaining the at least one self-installable package (Slivka '668: col. 2, lns. 54-55 – note that an immediate download and installation i.e. without taking time to negotiate a secure session, implies the user agreed to a non-secure session).

- (Claim 47) at least one of authenticating and decrypting the at least one self-installable package prior to installing the at least one self-installable package (Slivka '668: col. 13, lns. 16-26 – note that in an SSD exchange, the client re-verifies the transmitted package).
- (Claim 48) the instructions comprise an executable installation program plus one or more files to be installed (Slivka '668: col. 13, lns. 38-45 – note the Media Directive File controls the installation of the additional files).

Claims 50-51:

Regarding Claims 50-51, Slivka '688 and Meyerson '619, in combination disclose all the limitations of Claim 49 (supra). Additionally, Slivka '688 and Meyerson '619, in combination disclose:

- (Claim 50) negotiating a secure session prior to obtaining the at least one self-installable package (Slivka '668: col. 13, lns. 9-15; col. 2, lns. 65-67; col. 3, lns. 5-8);
- (Claim 51) the pre-determined entry comprise a file information subdirectory identifying installation instructions (Slivka '668: col. 13, lns. 38-45; col. 14, lns. 15-42 – note the Media Directive File reads on installation instructions; further note the directory specification for setup.exe, i.e. the setup executable).

Claim 54:

Regarding Claim 54, Slivka '688 and Meyerson '619, in combination disclose all the limitations of Claims 39, 40, 41, 42, 44, 45, 46, 47, 48, 49, 50, 51, 52, and 53 (supra).

Additionally, Slivka '688 and Meyerson '619, in combination disclose: a computer-readable storage medium holding code for performing the method according to Claims 39, 40, 41, 42, 44, 45, 46, 47, 48, 49, 50, 51, 52, and 53 (Slivka '668: col. 19, lns. 59-61). Slivka '668 does not

disclose all the limitations of Claim 43, however Examiner notes Claim 54 was written in the alternative, thus Claim 54 with respect to Claim 43 need not be addressed.

4. Claims 3 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slivka '668 and Meyerson '619 in view of U.S. Patent No. 5,978,912 issued to Rakavy et al. (hereafter Rakavy '912).

Claims 3 and 14:

Regarding Claims 3 and 14, Slivka '668 and Meyerson '619, in combination disclose all the limitations of Claims 1 and 12 (supra). However, Slivka '668 and Meyerson '619, in combination do not explicitly disclose: (Claims 3 and 14) a network operations center installing an initial set of installable components on each network appliance during a bootstrap configuration.

Rakavy '912 discloses: a network operations center installing an initial set of installable components on each network appliance during a bootstrap configuration (Rakavy '912: col. 4, lns. 4-14).

It would have been obvious to a person having ordinary skill in the art to apply the remote bootstrap of Rakavy '912 to the Slivka '668 and Meyerson '619 combination. The motivation to combine is suggested by Rakavy '912 which discloses the advantage that remote machines such as those of the Slivka '668 and Meyerson '619 combination, will be easier to administer, and further that diagnosing system failures will be enabled since the machines may be booted remotely independent of the operating system (Rakavy '912: col. 3, lns. 12-48).

Art Unit: 2161

5. Claims 24-25, 28-38, 43, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slivka '668 in view Meyerson '619 in further view of the publication "Understanding UPnP (TM): A Whitepaper" June 2000, published by the UPnP (TM) Forum (hereafter UPnP '00).

Claim 24:

Regarding Claim 24, Slivka '668 discloses: a system for autonomously managing a network appliance deployed within a distributed computing environment (Slivka '668: Abstract), comprising:

- an internal catalog of components installed on one such network appliance identified by component and version (Slivka '668: col. 7, lns. 39-44; col. 12, lns. 6-32 – note the Windows (TM) registry reads on an internal catalog of components); and
- periodically providing a status report: containing health and status information and application-specific data for the one such network appliance (Slivka '668: col. 2, lns. 37-43; col. 3, lns. 8-13; col. 3, lns. 21-23 – note that inventory and version information reads on health, status, and application specific data); and
- a catalog checker obtaining a catalog of currently installable components dynamically generated for the one such network appliance and determining noncurrent components by comparing the components and versions listed in the obtained catalog against the internal catalog (Slivka '668: col. 2, lns. 39-53).

However, Slivka '668 does not explicitly disclose that:

- the status report was from a status daemon "operating autonomously on the one such network appliance";

Art Unit: 2161

- the information is “pertaining to autonomous configuration and management”; or
- the catalog of currently installable components were “based on the status report independently received from the network appliance.”

UPnP '00 discloses the well-known Universal Plug and Play (TM) network management system which provides functionality for network clients to automatically notify other network entities of status, services, and other properties. Specifically, UPnP '00 discloses status reporting accomplished via a status daemon (UPnP '00: pp. 10-11, Section titled, “Devices”, and Section titled, “Services” – note that a UPnP (TM) enabled device contains a UPnP (TM) “device” which is a software container that exposes services and nested UPnP (TM) devices via UPnP (TM) protocols, and as such reads on a status daemon). However, UPnP '00 does not explicitly disclose:

- that the information is “pertaining to autonomous configuration and management”; or
- that the catalog of currently installable components were “based on the status report independently received from the network appliance.”

Meyerson '619 discloses an intelligent update agent. Specifically, Meyerson '619 discloses:

- that the information is “pertaining to autonomous configuration and management” (Meyerson '619: paras. [0028] and [0029]; paras. [0033], [0034], and [0036]); and
- that the catalog of currently installable components were “based on the status report independently received from the network appliance.” (Meyerson '619: paras. [0022] and [0026]).

It would have been obvious to a person having ordinary skill in the art to apply the status daemon of UPnP '00 to the Slivka '668 invention. The motivation to combine is suggested by UPnP '00 which discloses enabling a device to support UPnP (TM) by adding a UPnP (TM) device to expose services via UPnP (TM) protocols provide the advantage of making that device easier to setup and configure (UPnP '00: p. 1, Section titled, "What is UPnP (TM)?").

It would have been further obvious to a person having ordinary skill in the art to enhance the status daemon of UPnP '00 in the Slivka '668 and UPnP '00 combination with the autonomous intelligent update of the Meyerson '619 agent. The motivation to combine is suggested by Meyerson '619 which discloses the advantage that a class of updates that are critical to a machine need not rely on human interaction to initiate updates such as that of Slivka '668 and UPnP '00 combination (Meyerson '619: paras. [0011] and [0012]).

Claims 25, 28-29:

Regarding Claim 25-29, Slivka '668, UPnP '00, and Meyerson '619 in combination disclose all the limitations of Claim 24 (supra). Additionally, Slivka '668, UPnP '00, and Meyerson '619 in combination disclose:

- (Claim 25) a network operations center negotiating a secure connection with the one such network appliance (Slivka '668: col. 13, lns. 9-15; col. 2, lns. 65-67; col. 3, lns. 5-8);
- (Claim 28) a network operations center broadcasting a query message to each such network appliance to trigger a status report (UPnP '00: p. 11, Section titled, "Control Points" – note that on a UPnP (TM) enables system, a network operations center would have a UPnP (TM) control point, which provides the capability of querying UPnP (TM) devices for status reports);

- (Claim 29) the components comprise at least one self-installable package, further comprising: an installer obtaining the at least one self-installable package and installing the at least one self-installable package per instructions encoded therein (Slivka '688: col. 13, lns. 6-8; col. 13, lns. 27-37).

Claims 30-34, 37-38:

Regarding Claims 30-34, 37-38, Slivka '688, UPnP '00, and Meyerson '619 in combination disclose all the limitations of Claim 29 (supra). Additionally, Slivka '688, UPnP '00, and Meyerson '619 in combination disclose:

- (Claim 30) the components further comprise at least one file dependent on the at least one self-installable package, further comprising: an installer obtaining the at least one file subsequent to installing the at least one self-installable package and installing the at least one self-installable package per instructions stored in a pre-determined entry (Slivka '668: col. 13, lns. 38-45; col. 14, lns. 15-42 – note the Media Directive File reads on installation instructions; further note the directory specification for setup.exe, i.e. the setup executable);
- (Claim 31) a component server negotiating a non-secure session prior to obtaining the at least one self-installable package (Slivka '668: col. 2, lns. 54-55 – note that an immediate download and installation i.e. without taking time to negotiate a secure session, implies the user agreed to a non-secure session);
- (Claim 32) a crypto module at least one of authenticating and decrypting the at least one self-installable package prior to installing the at least one self-installable package (Slivka '688: col. 13, lns. 6-8; col. 13, lns. 27-37);

Art Unit: 2161

- (Claim 33) the instructions comprise an executable installation program plus one or more files to be installed (Slivka '688: col. 13, lns. 6-8; col. 13, lns. 27-37 – note the files comprising the installation read on at least one file);
- (Claim 34) the components further comprise at least one file, further comprising: an installer obtaining the at least one file and installing the at least one self-installable package per instructions stored in a pre-determined entry (Slivka '668: col. 13, lns. 38-45; col. 14, lns. 15-42 – note the Media Directive File reads on installation instructions; further note the directory specification for setup.exe, i.e. the setup executable);
- (Claim 37) at least one such network appliance performs one of electronic mail anti-virus scanning, content filtering, packet routing, and file, Web and print servicing (UPnP '00: p. 1, Section titled, "What is UPnP (TM)?" – note the references to "printing and imaging" as well as "proximity networks"; generally speaking UPnP (TM) enables an arbitrary network appliance);
- (Claim 38) the distributed computing environment is TCP/IP-compliant (Slivka '668: col. 6, lns. 26-28).

Claims 35-36:

Regarding Claims 35-36, Slivka '688, UPnP '00, and Meyerson '619 in combination disclose all the limitations of Claim 34 (supra). Additionally, Slivka '688, UPnP '00, and Meyerson '619 in combination disclose:

- (Claim 35) a component server negotiating a secure session prior to obtaining the at least one self-installable package (Slivka '668: col. 13, lns. 9-15; col. 2, lns. 65-67; col. 3, lns. 5-8);

- (Claim 36) the pre-determined entry comprise a file information subdirectory identifying installation instructions (Slivka '668: col. 13, lns. 38-45; col. 14, lns. 15-42 – note the Media Directive File reads on installation instructions; further note the directory specification for setup.exe, i.e. the setup executable).

Claim 43:

Regarding Claim 43, Slivka '668 and Meyerson '619 disclose all the limitations of Claim 39 (supra). However, Slivka '668 and Meyerson '619 do not explicitly disclose: broadcasting a query message to each such network appliance to trigger a status report.

UPnP '00 discloses: broadcasting a query message to each such network appliance to trigger a status report (UPnP '00: p. 11, Section titled, "Control Points" – note that on a UPnP (TM) enables system, a network operations center would have a UPnP (TM) control point, which provides the capability of querying UPnP (TM) devices for status reports).

It would have been obvious to a person having ordinary skill in the art to apply UPnP '00 to the invention of Slivka '668 and Meyerson '619 combination. The motivation to combine is suggested by UPnP '00. Specifically, UPnP '00 discloses the well-known Universal Plug and Play (TM) network management system which provides functionality for network clients to automatically notify other network entities of status, services, and other properties. Specifically, UPnP '00 discloses status reporting accomplished via a status daemon (UPnP '00: pp. 10-11, Section titled, "Devices" and Section titled, "Services" – note that a UPnP (TM) enabled device contains a UPnP (TM) "device" which is a software container that exposes services and nested UPnP (TM) devices via UPnP (TM) protocols, and as such reads on a status daemon).

Claim 52:

Regarding Claim 52, Slivka '668 and Meyerson '619 disclose all the limitations of Claim 39 (supra). However, Slivka '668 and Meyerson '619 do not explicitly disclose the network appliances perform at least one such network appliance performs one of electronic mail anti-virus scanning, content filtering, packet routing, and file, Web and print servicing.

UPnP '00 discloses the network appliances perform at least one such network appliance performs one of electronic mail anti-virus scanning, content filtering, packet routing, and file, Web and print servicing (UPnP '00: p. 1, Section titled, "What is UPnP (TM)?" – note the references to "printing and imaging" as well as "proximity networks"; generally speaking UPnP (TM) enables an arbitrary network appliance).

It would have been obvious to a person having ordinary skill in the art to combine network appliance variations of UPnP '00 with the Slivka '668 and Meyerson '619 combination. The motivation to combine is on the same basis as Claim 43 (supra).

6. Claims 26-27 and 41-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slivka '668, UPnP '00, and Meyerson '619, in view of the publication, "Plug-In Guide" published by Netscape Communications (TM), January 1998, as part of their browser plug-in SDK (hereafter Netscape '98).

Claims 26-27 and 41-42:

Regarding Claims 26-27 and 41-42, Slivka '668, UPnP '00, and Meyerson '619 in combination disclose all the limitations of Claims 24 and 39 (supra). However, Slivka '668, UPnP '00, and Meyerson '619 in combination do not explicitly disclose:

- (Claims 26 and 41) an initial plug-in executed on the one such network appliance;

- (Claims 27 and 42) a post plug-in executed on the one such network appliance;

Netscape '98 discloses a plug-in architecture for the Netscape Communicator (TM) browser. This architecture supports on-load and on-unload events with the NPP_INITIALIZE and NPP_DESTROY events as follows:

- (Claim 26 and 41) an initial plug-in execution (Netscape '98: "Reference to Functions by Functional Group", pp. 3-4 – note Section Labeled, "NPP_INITIALIZE");
- (Claim 27 and 42) a post plug-in execution (Netscape '98: "Reference to Functions by Functional Group", pp. 4-5 – note Section Labeled, "NPP_DESTROY").

It would have been obvious to a person having ordinary skill in the art to apply the plug-in architecture of Netscape '98 to the Slivka '668, UPnP '00, and Meyerson '619 combination. The motivation to combine is suggested by Netscape '98 which discloses that application of the plug-in architecture of Netscape '98 increases the flexibility of an application (Netscape '98: "Plug-In Basics", pp. 2-3 – note Section Labeled, "How You Can Use Plug-Ins").

Response to Arguments

7. Applicant's arguments filed September 29, 2004 have been fully considered but they are not persuasive. Applicant's arguments are addressed as follows:

- A. Addition of the Meyerson '619 reference addresses newly added limitations to Claims 1, 12, 24, and 39
(Amendment: p. 13, ln. 27 to p. 14, ln. 24; p. 16, ln. 8 to p. 17, ln. 10).

Examiner has added the Meyerson '619 reference to the rejections of amended Claims 1, 12, 24, and 39 to address the newly added limitations to amended as follows:

- an autonomous status daemon operating on the network appliance;
- information pertaining to autonomous configuration and management;
- configuration settings based on information independently received from the network appliance.

Mapping of Meyerson '619 to these new limitations are described in the rejections of Claims 1, 12, 24, and 39 (supra). Newly added Meyerson '619 reference was necessitated by Applicant's newly added limitations, and does not affect the finality of this Office Action.

B. Slivka '668 reads on "progressively assembled concurrent to" (Amendment: p. 14, lns. 6-12).

Slivka '668 recites a catalog server that reads on an update service (Slivka '668: col. 2, lns. 42-44). Furthermore, the catalog server of Slivka '668 is "capable of simultaneous access by a plurality of user computers (Slivka '668: col. 5, lns. 17-18). As a result, maintenance of the catalog operates independently, i.e. "is progressively assembled concurrent", across multiple accesses by various user computers.

Applicant discusses that the “catalog server can defer assembling configuration settings” (Amendment: p. 13, ln. 11). Note that while the catalog server of Slivka ‘688 initiates an update to a remote computer, it may concurrently receive data from another remote computer, and defer operations as it sees fit.

Additionally, it is noted that the features upon which applicant relies (i.e., the notion of deferral) is not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Finally, the claims as Amended are also addressed the addition of Meyerson ‘619. Since the intelligent update agent operates on the client machine separate from the server (Meyerson ‘619: paras. [0022] and [0026]), any “progressive assembling” by the catalog server is necessarily “concurrent to” operations by the update agent of Meyerson ‘619.

- C. Combination of Rakavy ‘912 is motivated, has reasonable expectation of success, and disclose all claim limitations of Claims 3 and 14 (Amendment: p. 15, ln. 24 to p. 16, ln. 7).

Examiner notes that Applicant merely asserts that the combination of Rakavy ‘912 is not motivated, does not have reasonable expectation of success, and does not disclose all claim limitations of Claims 3 and 14. Examiner reiterates prior

motivational statement, reasons for expectation of success, and mapping of limitations as set forth in the rejections of Claims 3 and 14 (*supra*).

- D. Addition of Meyerson '619 addresses newly added limitations inherited in Claims 26-27 and 41-42 (Amendment: p. 17, lns. 11-23).

Examiner refers Applicant to Argument A (*supra*).

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Patrick J.D. Santos whose telephone number is 571-272-4028. The examiner can normally be reached on M-F 8:00-4:30.

Art Unit: 2161

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Safet Metjahic can be reached on 571-272-4023. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Patrick J.D. Santos
February 3, 2005


FRANTZ COBY
PRIMARY EXAMINER